ALPHA BANK

ANTI-MONEY LAUNDERING AND COMBATING THE FINANCING OF TERRORISM (AML/CFT) POLICY

BANK's POLICY FRAMEWORK

The legalization of proceeds of criminal activities or "Money Laundering" (hereinafter "ML") refers to all activities intended to conceal the illegal source of funds. The financing of terrorism (hereinafter "FT") refers to activities intended to channel funds to third parties for terrorist purposes.

The solvency and the reputation of the Bank and the Group, as well as the reliability of the financial system in general, may suffer greatly as a result of the efforts made by criminals to conceal the source of the proceeds of criminal activities or to channel funds to terrorist activities.

Identifying the risks arising from ML and FT activities and their potential consequences, as well as the importance of combating financial crime, and taking also into account the provisions of the recommendations of the Financial Action Task Force (F.A.T.F.) and of the regulatory framework in force, the Bank has introduced and applied an Anti-Money Laundering and Combating the Financing of Terrorism Policy (AML/CFT Policy). This policy has been approved by the Board of Directors of the Bank.

More specifically:

With respect to procedures, these:

- Are adapted to the nature of the business activities of the Bank and comply with the local regulatory framework in force.
- Are assessed periodically and must be revised when deficiencies are identified or when the need arises to make adjustments.
- Are approved by the Board of Directors of the Bank and must be communicated to the Company's Staff, to whom duties and responsibilities are clearly allocated

With respect to IT systems, these:

- Are capable of providing timely and reliable information for controlling the clientele and the transactions, on the basis of the lists of persons or entities subject to sanctions, as such lists are issued by the various Authorities.
- Allow continuous monitoring and detection of transactions or activities which may be associated with ML or FT, using specific parameters (indicative typology of transactions, customer's financial/transactional profile, expected account activity etc.).

The Bank has appointed an AML/CFT Officer and an alternate thereof. The AML/CFT Officer is responsible for ensuring the proper and adequate implementation of the AML/CFT Policy.
The key components of the AML/CFT Policy are the following:

- Responsibilities of the AML/CFT Officer
- Customer Acceptance and Cooperation Policy
- Continuous Monitoring of Accounts and Transactions
- Reporting of Unusual/Suspicious Transactions
- Monitoring Bank's Compliance level to the Regulatory Framework

RESPONSIBILITIES OF THE AML/CFT OFFICER

The Manager of the Compliance Division has been appointed as responsible for ensuring the adherence of the Bank to all its AML and CFT obligations.

Within the Compliance Unit of the Bank an AML/CFT Special Service shall be established. The Board of Directors of the Bank shall ensure the independence of the AML/CFT Special Service.

CUSTOMER ACCEPTANCE POLICY AND POLICY FOR COOPERATION WITH CUSTOMERS

The Bank adopts a risk-based approach to the Policy and Procedures for assessing and effectively managing the risk of its services being used for ML and FT purposes.

A basic component of the Customer Acceptance Policy and the policy for cooperation with customers is the "Know Your Customer" (KYC) Principle which constitutes the basis of all AML/CFT procedures and covers the collection and maintenance of adequate information on a customer for the following purposes:

- Customer identification and verification
- Assessment of the customer's overall profile.
- Specific measures due diligence depending on the customer profile

The criteria used to assess customers are the following:

- The appearance of the customer in sanction lists.
- The information available for verifying the customer's identity.
- The customer's occupation or scope of activity.
- The legal form and the country of establishment of legal entities.
- The beneficial owner or beneficiary of the legal entity.
- The customer's country of origin or the country where the customer operates.
- The country of origin and destination of the funds.
- The volume, size and type of business transactions.
- The complexity of transactions.
- The use of new technologies in transactions.
- The deviations from the economic/transactional profile of the customer.

Categories of Unacceptable Customers

- Customers subject to prohibitions imposed by decisions of the European Union, UN, the national authorities of Cyprus or where Alpha Bank Group Companies are established or other international organisations.
- Customers (natural persons or legal entities) failing to provide all information required for the identification and verification of their identity.
- Customers for whom the collection of information for assessing their overall profile is impossible.
- Customers whose activities or transactions are not consistent with the information available on them, their professional activity, their risk profile and the origin of the funds.
- Customers for whom reports of unusual or suspicious transactions are repeatedly submitted to the local Financial Information Unit (FIU).
- Shell Banks.
- Shell Companies
- Gambling and betting companies (including companies with similar activities offered through the Internet) operating without authorization or supervision.
- Customers that appear to have betting and gambling activity on a regular basis.

- Customers active in the production / processing / marketing of prohibited products (weapons, weapons systems, ammunition, defense equipment, personal / nuclear products).
- Customers providing financial or insurance services without authorization or control by a supervisory authority.
- Foundations, Charities, Non-Profit Organizations operating without the necessary authorization in accordance with the Regulatory Framework
- Opening and maintaining secret, anonymous or unnumbered accounts, accounts with virtual names and accounts that do not display the full name of the beneficiary on the basis of their identity documents.

Categories of High-Risk Customers (Enhanced CDD)

- Customers subject to restrictions under decisions of the Office of Foreign Assets Control (OFAC), the Cyprus National Authorities and the Authorities of the countries where Alpha Bank Group Companies are established or other international organizations.
- Politically exposed persons.
- Companies with bearer shares.
- Offshore companies and Special Purpose Vehicles (SPVs).
- Deprived legal personality schemes or entities that manage funds or other asset groups: Trusts and foundations / non-profit organizations.
- "Customer Accounts" in the name of a third party (client's accounts).
- Cross-border correspondent banking relationships with third countries
- Clients originating from (final beneficiary country, country of registration) or operating in countries that are classified High Risk
- Investment Funds and Financial Services firms incorporated or operating in third countries.
- Payments and e-money service companies.
- Clients with unfavorable or negative information regarding ML/FT
- Customers questioned by Due Diligence Inquiries / Requests for Assistance / RFAs more than 2 times.
- Clients for whom the authentication process has not been completed
- Clients whose main purpose is to lend to other companies (usually in the same Group).
- Complex Business Structures
- Clients of International Activities where the final beneficiary is under 27 years of age.
- Clients with an increased risk of tax evasion.
- Clients active in areas considered as High Risk.
- Provision of banking services to Private Banking Customers
- Clients presenting unusually large, complex or unusual transactions.
- Customers with high cash flow activity.
- Customers classified in the PC category without necessarily fulfilling any of the above characteristics:
    - Clients at the discretion of the Compliance Officer
    - Clients at the discretion of the Relationship Manager

CONTINUOUS MONITORING OF ACCOUNTS AND TRANSACTIONS

Continuous monitoring of accounts and transactions is achieved by adhering to the relevant procedures, but mainly through appropriate IT systems.

The objective of continuously monitoring accounts and transactions is to detect unusual or suspicious transactions which as of their nature may be linked to ML/FT.